

The opinion in support of the decision being entered
today is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RONALD P. DOYLE

Appeal 2007-0231
Application 09/537,068¹
Technology Center 2100

Decided: September 21, 2007

Before KENNETH W. HAIRSTON, LEE E. BARRETT, and
ALLEN R. MacDONALD, *Administrative Patent Judges*.

BARRETT, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the final
rejection of claims 1-27. We have jurisdiction pursuant to 35 U.S.C. § 6(b).

We affirm-in-part.

¹ Application for patent filed March 28, 2000, entitled "Using
Biometrics on Pervasive Devices for Mobile Identification."

BACKGROUND

The claims are directed to a method, system, and computer program product for using biometrics on mobile pervasive devices for purposes of mobile identification. Mobile pervasive devices are mobile computing devices which are typically small, lightweight, and with a relatively limited amount of storage, such as cellular phones, programmable digital assistants (PDAs), handheld computers, etc. (Specification 1-2).

Claim 1 is illustrative:

1. A computer program product for using biometrics on pervasive devices for mobile identification, said computer program product embodied on a medium readable by said pervasive device and comprising:

programmable code means for capturing, using a biometric input reader which is attached to or incorporated within a mobile pervasive device possessed by a first party, biometric data of a second party; and

programmable code means for identifying said second party using said capture biometric data by comparing biometric data to previously-stored biometric data.

THE REFERENCES

Maes	US 6,016,476	Jan. 18, 2000
Crane	US 6,510,236 B1	Jan. 21, 2003
		(filed Dec. 11, 1998)

THE REJECTIONS

Claims 1-4, 7, 10-13, and 16 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Crane.

Claims 5, 6, 8, 9, 14, 15, and 17-27 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Crane further in view of Maes.

DISCUSSION

Claims 1 and 10

Arguments and rejection

Claims 1 and 10 recite "capturing, using a biometric input reader which is attached to or incorporated within a mobile pervasive device possessed by a first party, biometric data of a second party" and "identifying said second party using said capture biometric data."

Appellant argues that "it is clear that these distinct 'first' and 'second' parties are simultaneously involved when capturing biometric data and using this biometric data for identification" (Br. 8). It is argued that "Appellant finds no teaching in Crane that pertains to two distinct parties who are simultaneously participating in any action" (Br. 9). It is argued that Crane discusses validating the *user*, which is distinct from Appellant's *two-party* claim limitations (Br. 9-10).

We agree with Appellant that the Examiner misinterprets the argument about "simultaneously involved" to mean "simultaneously processing biometric data of two different parties" and finding this is not

claimed (Answer 7, 9, and 12). We agree with Appellant's reply (Reply Br. 2-4) that what is argued is that there are two parties simultaneously involved, the first party who possesses the mobile pervasive device and the second party whose biometric data is being captured.

The most relevant arguments by the Examiner are: (1) ownership or physical possession of a device is not a patentable distinction (Answer 8); (2) the device and system have no structural differences from the prior art and "the use of a device can not serve to distinguish a system, apparatus or product, if there [are] no structural differences" (Answer 11); (3) "apparatus or device claims must distinguish over the prior art in terms of structur[e] rather than function" (Answer 12); and (4) "[t]he limitation of possession, which is a descriptive term does not relate to nor does it affect the functionality and operations of the biometric pervasive device" (Answer 13-14) and does not limit the claim.

Appellant responds that the "identifying" limitation of claim 10 performs a different function than the authenticating taught by Crane (Reply Br. 6). "In particular, Appellant's 'identifying' limitation is for identifying 'said second party' who[se] biometric data has been captured -- and . . . this second party is not the device-possessing first party that is being authenticated by Crane" (Reply Br. 6).

Analysis

Claim 1 recites a "computer program product . . . said computer program product embodied on a medium readable by said pervasive device,"

which product comprises "programmable code means" for performing two functions. The "programmable code means" is interpreted to be instructions of a computer program stored on a tangible medium in the pervasive device. We interpret the limitations "for capturing" and "for identifying" to be functions to be performed when the program is executed on the pervasive device (i.e., executory functions), because what is claimed is a static computer program product, not a system or a method. The structures of the pervasive device and the biometric input reader are interpreted to be statements of the environment for the computer program product and not part of the claimed subject matter of the computer program product.

Claim 1 recites "programmable code means for identifying said second party using said captured biometric data by comparing biometric data to previously-stored biometric data," which requires that the comparison takes place on the pervasive device where the computer program product is stored. This apparently corresponds to the alternative embodiment described at Specification 16-17 where the pervasive device contains pre-stored biometric information. Claim 2 recites transmitting biometric data to a remote server, retrieving information using the biometric data, and returning the retrieved information to the pervasive device. Claim 2 corresponds to the description in the Specification where the comparison apparently takes place at the server (it is not expressly described that the transmitted biometric data is compared to biometric data at the server). It is not clear that claim 2 is consistent with and further limits claim 1 because claim 1

requires that the comparison of biometric data is done at the pervasive device where the program product is located, whereas claim 2 implies that comparison is done by server software. We leave the issue to be resolved by Appellant and the Examiner. For purposes of this appeal, we assume that claim 1 covers both remote and local comparison of biometric data.

There is another related claim language problem between claims 1 and 2. Claim 1 recites a "computer program product . . . said computer product embodied on a medium readable by said pervasive device." Claim 2 recites "programmable code means for retrieving, by said remote server, information from a repository using said transmitted biometric data; and programmable code means for returning said retrieved information to said mobile pervasive device" which requires two programmable code means at the server, which is inconsistent with the computer program product of claim 1 which is embodied on a medium readable by the pervasive device, not a system of software. We again leave the issue to be resolved by Appellant and the Examiner. Claims 10 and 11 do not have this problem because they are to a "system."

We conclude that the limitations "possessed by a first party" and "biometric data of a second party" are statements of intended use for the computer program product structure which do not limit the structure and are not entitled to any patentable weight. "There is an extensive body of precedent on the question of whether a statement of intended use constitutes a limitation for the purpose of patentability. Such statements often, although

not necessarily, appear in the claims preamble Whether a preamble of intended purpose constitutes a limitation to the claims is, as has long been established, a matter to be determined on the facts of each case in view of the claimed invention as a whole." (Citations omitted.) *In re Stencel*, 828 F.2d 751, 754, 4 USPQ2d 1071, 1073 (Fed. Cir. 1987). *See also Boehringer Ingelheim Vetmedica, Inc. v. Schering-Plough Corp.*, 320 F.3d 1339, 1345, 65 USPQ2d 1961, 1965 (Fed. Cir. 2003) ("An intended use or purpose usually will not limit the scope of the claim because such statements usually do no more than define a context in which the invention operates."); *Loctite Corp. v. Ultraseal, Ltd.*, 781 F.2d 861, 868, 228 USPQ 90, 94 (Fed. Cir. 1985) ("we interpret 'adapted to remain ... metal surfaces' as merely language of intended use, not a claim limitation"). What is claimed is structure: "programmable code means" stored on a tangible medium. Who is in "possession" of the mobile pervasive device and who is seeking to validate biometric data do not affect the structure. It is well known that the only way to claim a new use for a known structure is as a "process" under 35 U.S.C. § 100(b). *See 1 Chisum on Patents* § 1.03[8] (2003).

Crane inherently has programmable code means to capture biometric data and programmable code means to identify the person to allow access because it may be a mobile pervasive computing device which inherently runs on software (col. 4, ll. 24-28). Crane indicates that the comparison of captured biometric data to previously-stored biometric data is performed by the authentication device 16 in Figure 1 or the authentication controller 57 in

Figure 3, which then sends an identification of the device type (the "device-id"), as well as what user (the "id") is requesting access, to an application server 12 (col. 4, ll. 48-63). If the device is trusted, the application server 12 sends the authentication data to an authentication device server 18 (col. 4, l. 64, to col. 5, l. 27). The authentication device server 18 verifies the authentication data and provides a Yes or No to the application server 12, which knows if the user is to be given access and passes an authorization token to the user (col. 5, ll. 29-37). Thus, Crane discloses the claimed structure of a program embodied in the pervasive device for capturing and comparing biometric data to identify a person. This is not contested by Appellant. The limitation of "programmable code means for identifying said second party using said capture biometric data by comparing biometric data to previously-stored biometric data" in claim 1 does not exclude granting access to the pervasive device in response to the identifying a person as opposed to taking some other action.

The limitations of "possessed by a first party" and "biometric data of a second party" are not entitled to patentable weight because they do not affect the structure, but only recite an intended use for the structure. For example, if the owner of a pervasive device which uses biometric data to allow the owner access gives it to another person to hold while he or she enters the biometric data, the device is unchanged, but the device is "possessed by a first party" who holds the device and the owner is a second party who is identified by "biometric data of a second party." That is, who "possesses"

the device (legally or physically) and who is "identified" does not change the structure of the computer program product. The rejection of claim 1 is affirmed.

Claim 10 is also directed to structure and the limitations of "possessed by a first party" and "biometric data of a second party" are not given patentable weight because they do not affect the structure. The rejection of claims 10 is affirmed for the reasons discussed for claim 1.

Claims 3 and 12

Arguments and rejection

Claim 2 recites retrieving information from a remote server using the transmitted biometric data and claim 3 recites "wherein said retrieved information comprises a photograph of a party to whom said biometric data corresponds." Claim 12 contains the same limitation. Appellant argues that Crane does not teach these limitations and, in particular, the photograph is a photograph of the party, not a photograph of biometric data (Br. 13-14).

The Examiner characterizes Appellant's argument as saying that Crane does not teach the use of a photograph as biometric data (Answer 14). The Examiner provides a long discussion of the biometric operations (Answer 14-23). The gist of the discussion appears to be that photographs were a well known type of biometric data which is encompassed by Crane.

Appellant responds that the Examiner misinterprets the "photograph" in the claims. It is argued that the claim language does not specify use of photographs as biometric data and that "photographs" refers to conventional

photographs, used as a picture of a person (Reply Br. 6-7). It is noted that the photographs are retrieved based on the biometric data (Reply Br. 7).

Analysis

We agree with Appellant's arguments. The photograph is recited to be a photograph of a party to whom the biometric data corresponds. The photograph is not used as biometric data as understood by the Examiner. The photograph is retrieved in response to transmitted biometric data, which is not taught by Crane. Crane only returns an authorization token (col. 5, ll. 29-37). Thus, to the extent the nature of the biometric data (a photograph) is considered "nonfunctional descriptive matter," Crane does not return any biometric data. The rejection of claims 3 and 12 is reversed.

Claim 19

Arguments and rejection

Although claim 19 stands rejected under 35 U.S.C. § 103(a), it appears that the Examiner rejects it for the reasons stated with respect to claims 1 and 10 because the Examiner does not propose modifying Crane with any teaching of Maes. Appellant argues that claim 19 is patentable for the same reasons discussed with respect to claims 1 and 10, in particular, because there is no teaching of two distinct parties that can be aligned to the claimed "first party" and "second party" and because no text from Maes has been cited as teaching these distinct parties (Br. 16). The Examiner relies on the reasoning for claims 1 and 10 (Answer 23).

Analysis

It is well known that a "new use" of a known machine, manufacture, or composition of matter must be claimed as a "process" under 35 U.S.C. § 100(b). Whereas the statements of intended use were not entitled to patentable weight in the computer program product of claim 1 and the system of claim 10 because they did not limit the structure, the process format of claim 19 requires a slightly different analysis. The issue is whether the "use" limitations of "possessed by a first party" and "biometric data of a second party" patentably distinguish the method of claim 10 from the method performed by the apparatus of Crane. "A different use of a known substance, machine, or process is not 'new' within the meaning of this statute [§ 100(b)] if it merely analogous or cognate to the uses theretofore made." *Elrick Rim Co. v. Reading Tire Mach. Co.*, 264 F.2d 481, 486-87, 120 USPQ 514, 518 (9th Cir. 1959).

The limitation of "possessed by a first party" simply requires that the device is physically possessed by a person; it does not require legal ownership. Pervasive computing devices can be physically possessed by anyone, so this use limitation would at least have been obvious. The limitation of "biometric data of a second party" simply requires that another person, different from the first person, enter his or her biometric data. Again, nothing about pervasive computing devices limits who may enter biometric information, so this use limitation would at least have been obvious. For example, if you are showing off your pervasive computer

device to a friend and you enter your biometric data while he or she is holding it, the limitations are met. Or, if you are using a pervasive device which is the property of your employer, this satisfies the first person/second person limitation. The biometric verification device in Crane can be used for verification for any purpose by any party. Therefore, the rejection of claim 19 is affirmed.

Claims 8, 17, and 26

Arguments and rejection

The Examiner finds that Crane does not disclose a secure meeting where the coded means is used to identify attendees at a meeting. The Examiner finds that Maes discloses providing access to a secure building via a pervasive device at column 2, lines 50-58 (Final Rejection 4). Presumably, (because it is not expressly stated), the rejection is that it would have been obvious to use the pervasive device of Crane to control access to a secure building in view of the teachings of Maes.

Appellant argues that the cited portion of Maes does not pertain to "a plurality of meeting attendees" or a plurality of any other type of people, nor does it teach the two-party approach (Br. 17).

Analysis

Claim 8 presents the same issue of intended use as claim 1. The limitation that the computer program product "is used to enable on-demand creation of a secure meeting site by repeating operation of said

programmable code means for capturing and said programmable code means for identifying for each of a plurality of meeting attendees," is a statement of intended use for the device once a person has been identified and the use does not limit the structure of the "computer program product." That is, "repeating operation of said programmable code means for capturing and said programmable code means for identifying for each of a plurality of meeting attendees" is done by the programmable code means in Crane for each user authorized for access to the computer or the network resource. Allowing access to a meeting based on the outcome of the identification is not performed by the computer program product, but is simply a way that the outcome of the identification can be used. Claim 8 does not patentably distinguish over the computer program structure in Crane.

Although a further reference is not needed, Maes discloses using a pervasive device (a PDA) with biometric security to provide user verification (col. 2, ll. 31-34) to allow access to a building (col. 2, ll. 50-58), which would have motivated one of ordinary skill in the art to control access to a building based on biometric identification. The building is considered a secure meeting site because verification is necessary to enter. Claim 8 does not patentably distinguish over the computer program structure in Crane or the use of the device in Crane to control access to a building as taught by Maes. The rejection of claim 8 is affirmed. Claims 17 and 26 contain similar limitations and the rejection of claims 17 and 26 is also affirmed.

Claims 9, 18, and 27

Arguments and rejection

The Examiner finds that Crane does not disclose transmitting a trusted message. The Examiner finds that Maes discloses transmitting trusted messages at column 2, lines 23-67, column 3, lines 15-35, and 40-67. Presumably, (because it is not expressly stated), the rejection is that it would have been obvious to use the pervasive device of Crane to transmit a trusted message in view of the teachings of Maes.

Appellant argues that the cited portion of Maes does not pertain to "biometric data of a second party" or a "second party [who] is a potential recipient of [a] trusted message," but relates to utilizing biometric security to provide user verification (Br. 18). It is argued that Maes does not teach a two-party approach as claimed in the claims from which claims 9, 18, and 27 depend (Br. 18).

Analysis

Again, claim 9 presents the issue of intended use. Claim 9 recites that "said computer program product is used to exchange a trusted message by performing operation of said programmable code means for capturing and said programmable code means for identifying wherein said second party is a potential recipient of said trusted message." The only structural limitations are the programmable code means for capturing and the programmable code means for identifying. The exchange of a trusted message is not required to be performed by operation of the computer program product as disclosed in

the Specification, pages 13-14, where the possessor of the pervasive device decides whether to deliver a message depending on the identification. Thus, the use does not structurally limit the computer program product and is not entitled to patentable weight.

Although a further reference is not needed, Maes discloses using a pervasive device (a PDA) with biometric security to access confidential information (col. 2, ll. 31-34, 50-58), which is another way of saying exchanging a trusted message. Claim 9 does not patentably distinguish over the computer program structure in Crane or the use of the device in Crane to control access to information as taught by Maes. The rejection of claim 9 is affirmed. Claims 18 and 27 contain similar limitations and the rejection of claims 18 and 27 is also affirmed.

Claim 21

Claim 21 is rejected for the same reasons as stated for claims 3 and 12. For the reasons discussed in connection with claims 3 and 12, the rejection of claim 21 is reversed.

Claims 2, 4-7, 11, 13-16, 20, and 22-25

Appellant states that dependent claims 2, 4-7, 11, 13-16, 20, and 22-25 stand or fall with the independent claims from which they depend (Br. 15; Br. 20). Because these claims depend on rejected claims whose rejection has been affirmed, the rejection of claims 2, 4-7, 11, 13-16, 20, and 22-25 is affirmed.

Appeal 2007-0231
Application 09/537,068

CONCLUSION

The rejections of claims 1, 2, 4-11, 13-20, and 22-27 are affirmed.

The rejections of claims 3, 12, and 21 are reversed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv) (2006).

Appeal 2007-0231
Application 09/537,068

AFFIRMED-IN-PART

eld

MARCIA L. DOUBET LAW FIRM
P.O. BOX 422859
KISSIMMEE, FL 34742